논문 99-24-3A-10 한국통신학회논문지 '99-3 Vol.24 No.3A

개선된 DES의 고속 암호칩 구조 설계

정회원 최 광 윤*, 정 일 용**, 한 승 조***

Design of architecture for the High Speed Encryption Chip of Improved DES

Kwang-Yun Choi*, Il-Yong Chung**, Seung-Jo Han*** *Regular Members*

요 약

DES 알고리즘을 대체할 수 있는 112비트의 키 길이를 갖는 개선된 DES 알고리즘은 논문 [1]과 [2]에서 발표되었다. 개선된 DES는 평문을 96비트로 입력받고, 이것을 각각 32비트의 3개의 서브블록으로 분리한다. S-box는 8개에서 16개로 증가되었으며, 3개의 서브블록에 있는 f함수들이 비대칭적으로 수행되기 때문에 differential cryptanalysis 공격에 DES 보다 강하다.

본 논문은 개선된 DES를 하드웨어로 설계하는데 있어서 고속의 병렬 파이프라인 구조를 제안하고 VHDL로 기술하여 시뮬레이션 함으로써 초고속의 블록 암호화 시스템을 구현하였다. 설계된 하드웨어는 병렬 파이프라인의 구조를 갖으며, 파이프라인의 크기는 83단계로 매우 크게 설계되어 있다. 따라서 대량의 데이터나 스트림형 통신망에서의 암호화에 적합한 구조이며, 시뮬레이션 결과 입력클록 350MHz에서 33.33Gbps의 초고속 암호화 속도를 갖는다.

ABSTRACT

The Improved DES algorithm had been published as a replacement to the Data Encryption Standard(DES) in [1] and [2]. It has a key length of 112 bits. The plaintext data consists of 96 bits divided into 3 sub-blocks with 32 bits. The Improved DES has a potentially higher resistance to differential cryptanalysis than the DES due to the asymmetric number of f functions performed on each of the 3 sub-blocks and due to the increase of S-boxes from 8 to 16.

We have designed the Improved DES as hardware using the high-speed parallel pipeline structure first. And then we have performed the simulation of the ultra high-speed block cipher system described by VHDL. Designed hardware has parallel pipeline structure, pipeline depth is 83 step that is very large step. Therefore, the structure was compatible in large data or stream data communication network. As result of the simulation, we could got the high speed encryption chip of 33.33Gbps at the input pulse of 350MHz.

I. 서 론

컴퓨터 통신의 발달로 개인적이고 독립적이던 정보들이 개인 또는 국가간의 상호교류가 개방화되고 수월해짐에 따라 기업이나 국가의 존폐를 위협할 수 있는 요소로까지 치닫게 되었다. 이에 다가오는 2000년은 정보와의 전쟁이라고 전망하고 있으며 이 정보는 빠른 통신망을 타고 국경의 장벽을 넘어 초국가적인 재화로 인정받을 것이다. 따라서 유형적인 물질의 가치보다는 무형적인 정보의 가치가 중요한 정보화 시대를 맞이하여 제 3자의 공격에 대한 정보의 보호가 중요한 이슈로 등장하게 되었다.

* 조선대학교 전자공학과 ** 조선대학교 컴퓨터공학부 *** 조선대학교 전자·정보통신공학부

논문번호 : 98507-1121, 접수일자 : 1998년 11월 21일

※ 본 논문은 한국과학재단지정 지역협력연구센터인 조선대학교 수송기계부품공장자동화연구센터의 연구비지원에 의해 연구되었음

정보의 보호에 가장 많이 사용되는 방법으로 정보의 암호화를 들 수 있으며, 호주, 일본 등 세계의 각국들이 자국의 암호화 알고리즘을 개발하여 실용화하고 있는 실정이다. 또한 정보화기기의 고속화에 따른 고속의 암호화기가 필요해지게 되었고, 수십 Mbps에서 1.5Gbps의 암호화 속도를 갖는 여러 상업용 암호화 소프트웨어 및 하드웨어 제품들이 개발되고 있다. 실제로 반도체 기술이 발달하여 IC의 패킹밀도가 증가하면서 암호화 알고리즘의 칩 구현이 활발히 진행되고 있으며, 고속화에 따른 암호알고리즘의 공격 가능성이 높아지고 공격방법도 다양해지게 되었다.

최근에 암호화 제품들은 특별한 형태의 하드웨어로 구현되어지고 있다. 암호화와 복호화 박스는 통신라인에서 플러그 형식으로 삽입할 수 있으며, 통신라인을 통하는 모든 데이터는 암호화되어진다. 암호화 시스템에서 하드웨어는 아직까지 상업용이나 군사용이 대부분이며, 그 외에는 소프트웨어로 구현되었다. 그러나 다음의 몇가지 이유로 인하여 하드웨어 제작이 필요해지고 있다.[3]

첫째, 속도가 빠르다. 암호화 알고리즘은 암호강도를 높이기 위해 비트열들에 대한 많은 연산을 수행한다. 따라서 많은 연산으로 인해 수행시간이 길어지므로 소프트웨어로 구현할 시에는 수행속도에 문제가 있지만 하드웨어는 수행속도가 빠르기 때문에 이러한 문제를 해결할 수 있다.

둘째, 보안이 우수하다. 소프트웨어로 기술된 암호 알고리즘은 물리적인 보호가 되지 않으나, 하드웨어는 캡슐화 된 패키지에 넣어 보호를 할 수 있다. 특별하게 제작된 VLSI 칩은 칩의 로직을 분해함으로써 내부 구조를 분석하려는 시도를 화학적으로 막아낼 수 있다.

셋째, 설치가 간편하다는데 있다. 암호화가 범용 컴퓨터에만 적용되지는 않고 전화나, FAX 또는 데이터 전송에도 적용되는데, 이러한 경우에는 소프트웨어보다는 하드웨어 시스템의 구현 및 설치가 더 효율적임을 의미한다.

개선된 DES에 대한 알고리즘은 DES와 비교하여 암호강도 및 differential cryptanalysis[4]에 더 강하다는 것을 논문 [1]과 [2]에서 분석 및 평가하였다. 따라서 본 논문에서는 분석 및 평가가 이루어진 개선된 DES의 알고리즘에 대하여 VHDL을 이용하여 고속의 동작이 가능한 병렬 파이프라인구조를 제안하고, 하드웨어로 설계하여 초고속의 블록 암호화 시스템을 구현하고자 한다. 파이프라인 처리는 선형성을 갖는 연산과정을 몇 개의 단계로 구분하여 각 단계가 중첩되어 동시에 수행되도록 함으로써 명령어의 수행이 끝나기 전에 다른 명령어의 수행을 시작하는 연산 방법이다. 따라서 블록간에 독립적이며 데이터의 흐름이 선형적인 개선된 DES의 16라운드에 대한 파이프라인 처리는 효과적이다.

제안된 구조는 83단계의 파이프라인을 갖으며 각 단계가 2개의 서브프로세스블록으로 구성되어 있다. 각각의 서브프로세스블록은 서로 독립적이며, 1단계의 지연을 두고 동작하게 구성하여 각 서브프로세서에서 필요로 하는 테이블들을 절반으로 줄이는 방법을 적용하였다.

Ⅱ. 개선된 DES 알고리즘

1. 기본구조

DES는 왼쪽과 오른쪽 서브블록들이 16라운드 동안 동일한 횟수의 f 함수를 수행한다.[5] 따라서 DES를 확장할 때 암호학적 공격에 더 견고하게 하기 위해서는 16라운드의 각 서브블록동안 서로 다른 f 함수를 적용하는 등의 구조상의 변경이 필요하다. 이것을 위하여 96비트 한 블록의 데이터를 32비트의 3개의 서브블록으로 분할함으로써 비대칭으로 만든다.

$$B_i = C_{i-1} \oplus f(B_{i-1}, K_i)$$

$$C_i = A_{i-1} \oplus f(B_{i-1}, K_i) \qquad (1)$$

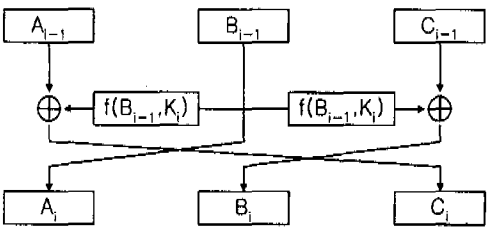


그림 1. 개선된 DES의 구조 (1라운드)
Fig. 1 Structure of Improved DES (1 round)

이것을 초기조건 $C_i = B_{i-1}$ 와 같이 단순화시켜 적용하여 보면, 완전히 같은 특성으로 반대편에 위치함을 알 수 있다. 식(1)에 의한 조합은 대칭적이며, 따라서 본 개선된 DES 알고리즘에서 그림 1과 같이 적용하였다. 암호화와 복호화는 각각의 관계를 서로 비교함으로써 동치임을 확인할 수 있다. 그림

1로부터 암호화 공식을 유도하면 다음과 같다.

$$A_i = B_{i-1}$$

$$B_i = C_{i-1} \oplus f(B_{i-1}, K_i) \quad (2)$$

$$C_i = A_{i-1} \oplus f(B_{i-1}, K_i)$$

식 (2)로부터, XOR 특성과
$f(B_{i-1}, K_i) = f(A_i, K_i)$를 이용하면 다음의 복호화 식을 얻는다.

$$B_{i-1} = A_i$$

$$C_{i-1} = B_i \oplus f(A_i, K_i) \quad (3)$$

$$A_{i-1} = C_i \oplus f(A_i, K_i)$$

A와 B를 서로 바꾸면 다음과 같은 관계를 얻을 수 있다.

$$A_{i-1} = B_i$$

$$B_{i-1} = C_i \oplus f(B_i, K_i) \quad (4)$$

$$C_{i-1} = A_i \oplus f(B_i, K_i)$$

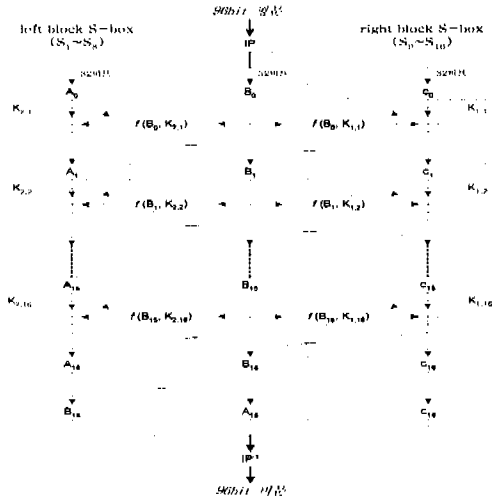


그림 2. 개선된 DES의 암호화 알고리즘
Fig. 2 Encryption algorithm of improved DES

식 (4)에 보여진 것과 같이 복호화 식도 식 (2)와 같은 구조를 이루고 있다. 그러므로 하나의 하드웨어로 암호화와 복호화를 같이 적용할 수 있다. 개선된 DES의 암호화 알고리즘이 그림 2와 같으며 3개의 32비트 서브블록으로 나누어진다. 또한 초기순열 (IP)과 역초기순열 (IP-1)도 96비트로 확장되었다.

f 함수는 각 구조에서 왼쪽과 오른쪽에서 동작하며, 왼쪽과 오른쪽 각각에서 f_1과 f_2로 명명되어 있다. S-box의 수는 16개로 증가시키는데, S_1에서 S_{16}까지로 명명되며 왼쪽 f 함수에 S_1에서 S_8, 오른쪽 f 함수에 S_9에서 S_{16}이 사용된다. 마지막으로 식을 적용하는데 있어서 암호화의 마지막 라운드 결과인 A_{16}과 B_{16}은 서로 교환되어야 한다.

공식에 의한 개선된 DES의 복호화 알고리즘이 그림 3과 같다. 복호화 알고리즘은 암호화 알고리즘과 같으나 첫 번째 라운드에서 A_0와 B_0를 서로 바꾸어 주어야 한다. 각 라운드의 서브블록에 다른 f 함수를 가지기 위하여 입력키를 64비트에서 128비트로 확장하였다. 16개의 패리티비트를 제거한 후 남은 입력키는 왼쪽의 K_1과 오른쪽의 K_2로 각각 56비트씩 2개의키로 나눈다. 또한 PC-1(Permuted Choice 1)을 거친 후 56비트의 키는 좌우로 28비트씩 나뉘어 지고, 매 라운드 동안 K_1과 K_2는 키 스케줄에 따라 왼쪽으로 쉬프트 된다. 각 라운드에 해당하는 키의 56비트 출력은 PC-2(Permuted Choice 2)를 통과한 후 48비트로 줄어들고, 왼쪽과 오른쪽 각각 $K_{1,i}$와 $K_{2,i}$로 명명된 후 각 라운드에 적용된다. (i=0 to 16)

2. 관리 및 f 함수

복호화 과정의 키는 암호화 과정에서 적용된 키와 반대로 입력되어야 한다. 또한 S-box도 왼쪽과 오른쪽이 서로 바뀌어야 한다.

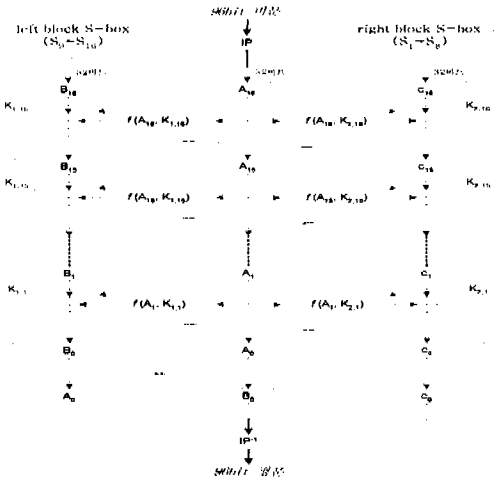


그림 3. 개선된 DES의 복호화 알고리즘
Fig. 3 Decryption algorithm of improved DES

개선된 DES가 differential cryptanalysis에 보다 견고하게 하기 위하여 f함수의 수를 증가시켰다. 증가된 수치는 3개의 서브블록과는 차이가 있다. 본래의 DES에 사용된 f 함수는 R_0에서 L_{16}까지 그리고 L_0에서 R_{16}까지 변환되는 과정에서 8번 반복된다. 반면에 개선된 DES의 f 함수는 A_0에서 C_{16} 까지 처리될 때 11번 반복된다. 이것은 같은 E(Bit-selection table), P(Permutation table) 그리고 S-box에서 개선된 DES가 본래의 DES에 비해 differential cryptanalysis에 보다 더 견고함을 보여준다.

3. S-Box

S-Box의 설계는 알고리즘의 강도에 결정적인 영향을 미친다. DES에 있어서 비선형적인 모듈러-2 알고리즘이 단지 하나의 단계에 불과한 반면 실제적인 알고리즘의 암호강도는 S-Box에 의존하고 있다.[6] S-Box의 엔트리를 개선하기 위해 DES는 잘 분석된 엔트리를 사용한다. 이 분석은 평균비트확률($P_{i,j}$)과 그 상호계수[6]에 의해 나타나는 SAC(Strict Avalanche Criterion)[7]에 근거하고 있다.

Ⅲ. 알고리즘의 고속 병렬파이프라인구조 설계

본 논문에서 설계한 개선된 DES는 크게 초기치환(IP), 16회 반복 라운드 그리고 역초기치환(IP^{-1})으로 나눌 수 있으며, 16회 반복되는 라운드를 전부 선형적으로 구현하게 되면 그림4의 구조를 이룬다.

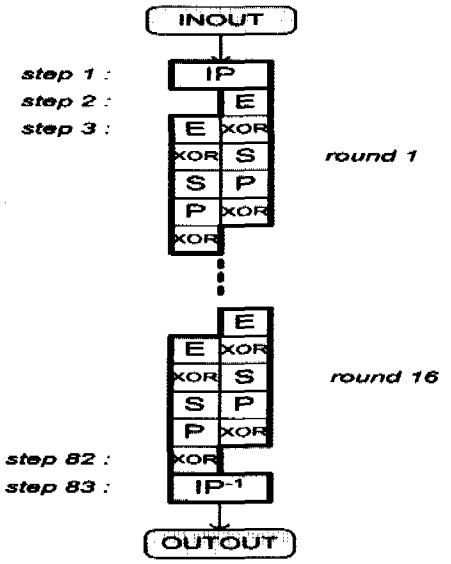


그림 4. 개선된 DES의 파이프라인구조
Fig. 4 The pipeline structure of imporved DES

각 라운드는 좌우측이 각각 E, XOR, S, P 그리고 XOR 등 5단계로 구성되어 있으나 1단계 지연을 두고 동작한다.[8,9] 따라서 한 라운드는 6개의 단계를 갖는다. 이때 16라운드를 전부 선형으로 연결하면 각각의 단계에서 1단계는 다음 단계와 중복되어도 되기 때문에 16라운드 전체는 5*16+1 개의 단계를 갖게 되고 여기에 IP와 IP^{-1}을 추가하여 총 83단계의 파이프라인 구조를 가지게 된다. 설계된 83단계의 파이프라인 구조가 그림 5에 나타나 있다.

개선된 DES는 96비트의 데이터 입력을 갖게 되며, 3개의 32비트 블록들로 분할되어 16회 단일 라운드를 수행하게 된다. 이때 좌측 서브프로세싱블록과 우측 서브프로세싱블록은 서로 독립적으로 동작하므로 우측보다 좌측을 1스텝씩 지연을 시킴으로써 치환이나 대치연산에서 사용되는 테이블을 32개에서 16개로 줄일 수 있으며, 전체 블록도는 그림 5와 같다.

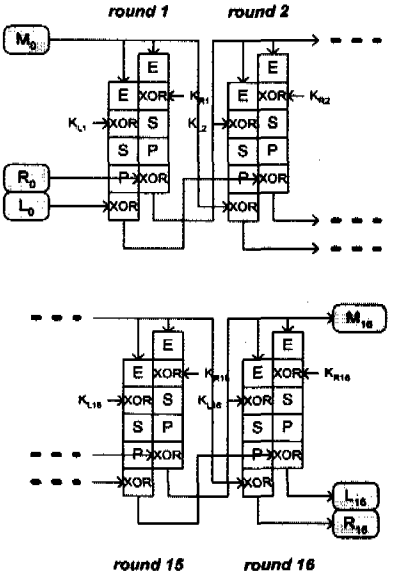


그림 5. 개선된 DES의 전체 블록도
Fig. 5 The block diagram of improved DES

좌우측 각각의 서브프로세싱블록들은 서브키 K_l과 K_r을 입력으로 갖으며 총 32개의 서브키를 사용한다.

Ⅳ. 칩 설계 및 시뮬레이션

1. 칩 설계

개선된 DES의 설계는 Round Block, Key Block 그리고 Control Block 등 크게 3부분으로 나누어진

다. Round Block은 개선된 DES의 병렬 파이프라인구조를 이루고 있는 블록이며 2분주 된 Clk에 의해 각종 Table을 공유하고 있다. Key Block은 16라운드에서 사용될 K_1과 K_2를 생성하는 블록으로 데이터의 입력 전에 미리 입력키를 이용하여 각 라운드의 서브키를 생성해 놓는다. 생성된 서브키는 Key Register에 보관되어 있게 되며 새로운 키가 입력되기 전까지 계속 유지된다. Control Block은 Key Block과 Round Block이 유기적인 동작을 할 수 있도록 외부 제어선의 제어하에 내부 각 블록들을 세부적으로 제어하는 블록이며, 마지막 데이터의 파이프라인에서의 현재위치 등을 계산하는 기능을 갖는다.

1.1 Round Block

라운드 블록은 입력된 데이터를 16라운드의 개선된 DES 알고리즘을 실질적으로 처리하는 블록으로 데이터는 96비트로 입력받아 96비트로 출력한다. 외부의 제어선인 op가 상승에지일 때 초기순열(IP)은 데이터 버스로부터 값을 입력받아 초기순열을 수행한 후 데이터를 첫 번째 라운드의 입력으로 보낸다. 각 라운드에서 좌우측이 각각 5개의 스테이지로 구성되어 있으면서 1단계 엇갈리게 구성되므로 각 라운드 전체는 6개의 스테이지로 이루어지게 된다. 따라서 16개의 라운드는 83개의 스테이지로 이루어지며 매 클록(clk)마다 한 단계씩 진행한다. 각 라운드에서 좌측과 우측의 스테이지들은 서로 같은 클록에 같은 테이블을 요구하지 않으므로 각각의 테이블들을 공유할 수 있다. 그림 6은 라운드블록의 블록도이다.

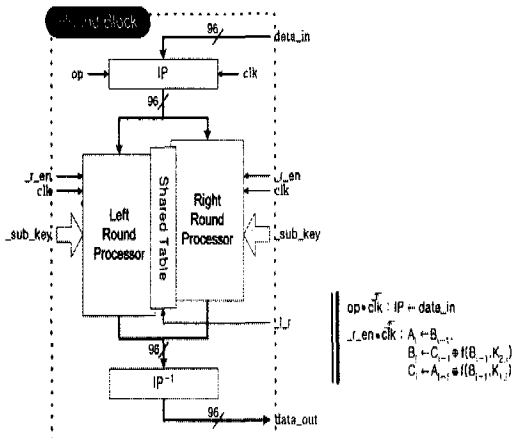


그림 6. Round Block의 블록도
Fig. 6 The block diagram of Round Block

각 라운드에는 키 블록으로부터 미리 생성되어 있던 서브키가 입력이 되며 _r_en이 엑티브 일 때 클록(clk)의 상승 에지에서 제공된 서브키를 이용하여 한 스테이지씩 암호화를 수행한다. 암호화 과정에서 공유되는 테이블은 _l_r 선택시그널에 의해 좌측라운드에서 사용할 것인지 우측라운드에서 사용할 것인지 결정된다.

83단계를 모두 거친 데이터는 역초기순열(IP^{-1})을 거쳐 96비트의 데이터 버스를 통해 출력된다. 그림 7은 라운드블록을 합성한 결과이다.

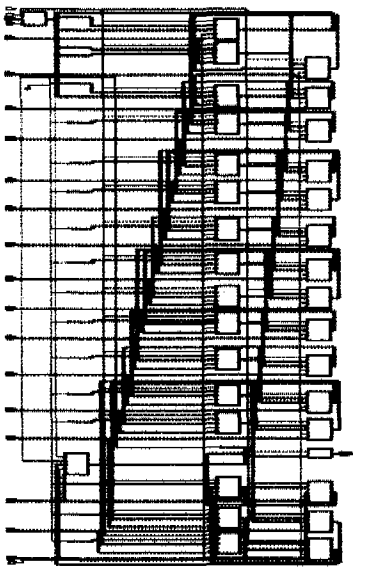


그림 7. 라운드블록의 합성결과
Fig. 7 Synthesis result of round block

1.2. Key Block

키 블록은 입력된 128비트의 키를 PC-1을 통해 패리티 비트를 제거하여 112비트로 줄인 후 키 스케줄에 따라 라운드별로 좌측 쉬프트를 수행한 후 PC-2를 거쳐서 키 레지스터에 저장한다. 키 레지스터는 16라운드에 해당하는 좌측 서브키와 우측 서브키를 보관하고 있게 된다. 키의 입력은 외부제어선인 key_in에 의해 이루어진다.

라운드블록의 1단계 지연설계에 따라 좌측과 우측이 키를 동시에 필요로 하지 않기 때문에 서브키의 출력 net를 좌·우측이 공유할 수 있다. 출력될 좌·우 서브키는 _l_r에 의해서 선택되며 컨트롤 블록에 의해 제어된다. enc 제어시그널은 키가 출력될 때 현재의 동작이 암호화에 따른 정순 출력인지 복호화 처리에 따른 역순 출력인지를 지시한다. 그림 8은 키 블록의 블록도이다.

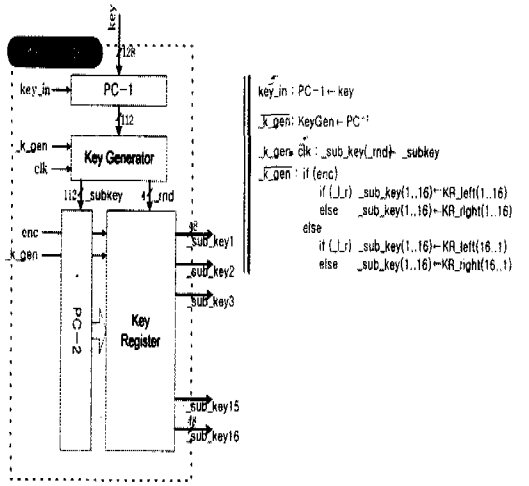


그림 8. Key Block의 블록도
Fig. 8 Block diagram of Key Block

라운드 블록에서 사용되는 키는 다음의 새로운 키가 입력될 때까지 내부 레지스터에 유지되며, 키 제너레이터는 _k_gen이 액티브일 때 클록(clk)에 따라 내부 카운터가 1부터 16까지 증가하면서 서브키를 생성하여 키 레지스터로 전송하게 된다.

키 블록의 합성결과가 그림 9에 나타나 있다.

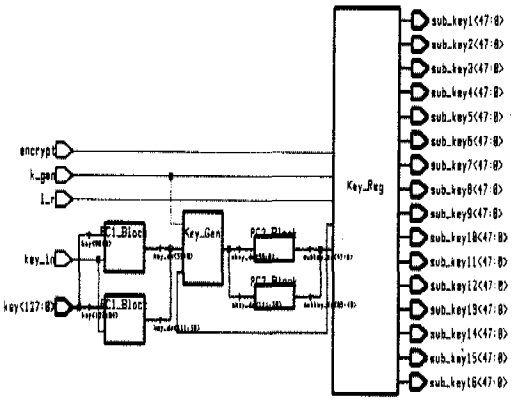


그림 9. 키블록의 합성결과
Fig. 9 Synthesis result of Key Block

1.3. Control Block

컨트롤 블록은 크게 2가지의 기능을 갖는다. 첫째, 외부의 제어선으로부터 입력을 받아 전체 블록들을 제어하는 기능과, 둘째, 입력된 데이터가 몇 번째 단계를 수행 중인지를 카운트하여 최종 데이터가 중간단계에 잔류하지 않도록 하는 기능으로 분류된다. 컨트롤 블록의 블록도가 그림 10에 나타나 있다.

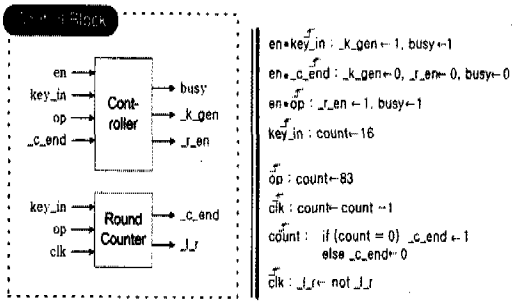


그림 10. Control Block의 블록도
Fig. 10 Block diagram of Control Block

컨트롤 블록은 현재 데이터가 중간의 단계에 아직 남아 있을 경우 busy 신호선을 액티브 상태로 유지한다. 그리고 마지막 데이터가 출력이 된 후에는 _c_end 신호선이 액티브 되어 busy 신호선을 not busy로 유도한다. 컨트롤 블록의 합성결과는 그림 11과 같다.

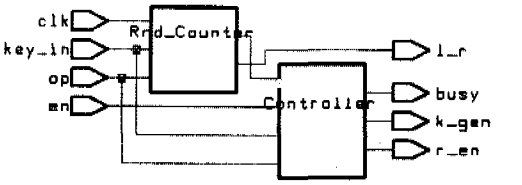


그림 11. 컨트롤블록의 합성결과
Fig. 11 Synthesis result of Control Block

2. 시뮬레이션

개선된 DES는 데이터의 입력을 96비트로 하고 112비트의 키를 필요로 하는 블록 암호화 알고리즘으로 암복호화 과정을 검증하기 위하여 다음과 같은 조건에서 시뮬레이션을 수행하였다.

- Key : t"InfoCommSystem"
  (49 6e 66 6f 43 6f 6d 6d 53 79 73 74 65 6d)
- Data : "DESCHIP-FPGA"
  (44 45 53 43 48 49 50 2d 46 50 47 41)
- Clock : 350 MHz
- Simulator : Active-VHDL

적용된 키는 고정으로 유지하고 입력데이터는 96비트를 83회 반복해서 입력하였다. 83개의 스테이지를 모두 거쳐 암호화된 출력데이터를 다시 복호화 과정의 입력으로 넣어 여기서 출력된 복호화 된 데이터가 원본과 일치함을 확인하였다. 암호화 및 복호화 시뮬레이션 결과는 그림12, 그림13과 같다.

또한 대형 스트림 데이터에 대한 시뮬레이션 결

과가 그림 14에 나타나 있다. 적용된 데이터로 229KB 크기의 그림 15(합성결과 이미지 데이터)를 사용하였으며, 암호화 후 복호화한 파일을 그림 15에 사용한 것이다. 그림 14에 보여지는 것처럼 229KB의 시뮬레이션 결과 입력클록 350MHz에서 약 50μ s의 소요 시간을 나타내고 있다.

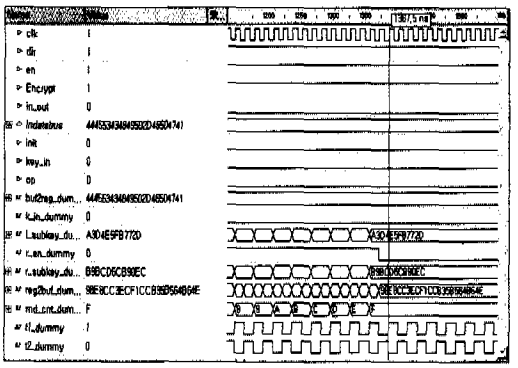


그림 12. 개선된 DES의 암호화 시뮬레이션
Fig. 12 Encryption Simulation of improved DES

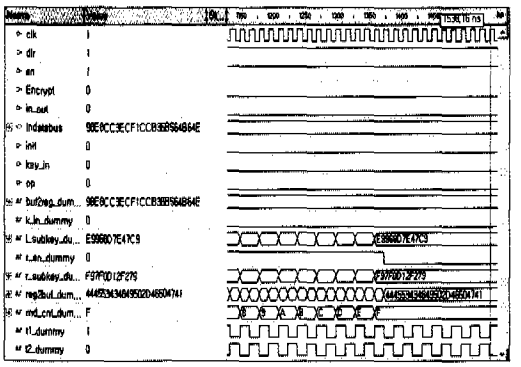


그림 13. 개선된 DES의 복호화 시뮬레이션
Fig. 13 Decryption Simulation of improved DES

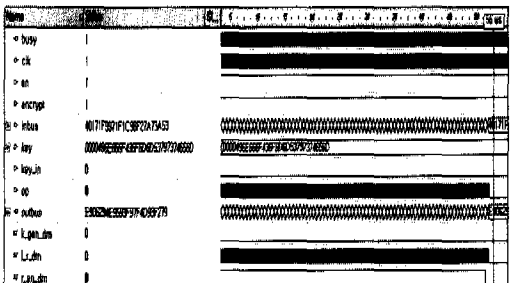


그림 14. Stream 데이터의 시뮬레이션
Fig. 14 Simulation of Stream Data

전체시스템에 대한 합성결과는 그림15와 같다.

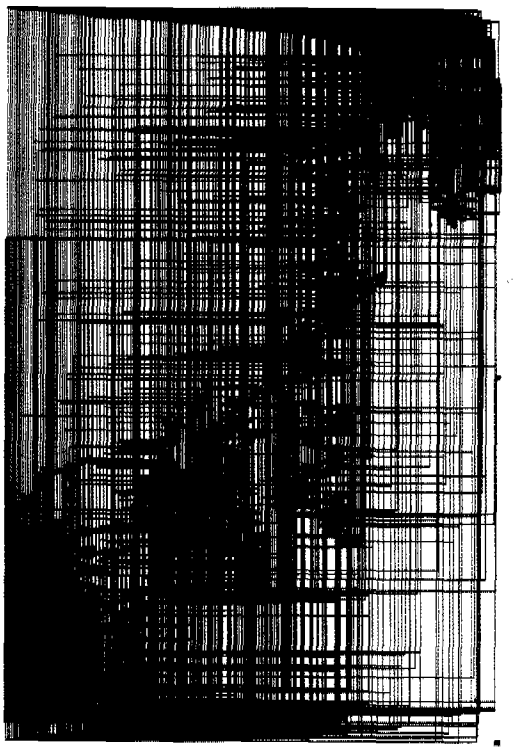


그림 15. 개선된 DES의 전체 합성 결과
Fig. 15 Synthesis result of improved DES

V. 분석 및 고찰

암호화 과정은 앞에서 언급한 바와 같이 83단계의 파이프라인으로 구성된다. 이렇게 긴 단계가 가능한 것은 암호화 전과정이 분기가 없기 때문이며 긴 데이터의 입력일수록 파이프라인의 효과가 크다. 즉, 96비트 한 블록을 일반적인 비 파이프라인으로 처리하거나, 본 논문에서 제안한 83단계의 블록을 한 단계로만 처리하게 될 경우 성능의 향상은 단지 하드웨어로 구현한 병렬처리 효과밖에 없게 된다. 이 경우 96비트 한 블록을 암호화하는데 소요되는 사이클 수는 각 단계별로 1 사이클씩 총 83사이클이 필요하다. 본 논문에서 제안한 83단계 파이프라인은 96비트의 블록을 계속해서 순차적으로 파이프라인에 넣었을 때 83단계가 모두 채워질 때까지는 한 블록으로 처리했을 때와 같기 때문에 한 블록 암호화하는데 소요되는 사이클 수는 83 사이클로 앞의 경우와 같게되나 입력된 블록들이 많으면 많을수록 1사이클에 근접하게 된다. 이것은 기존의 단

일블록 처리 때보다 약 83배의 성능향상을 가져오게 된다. 따라서 본 논문에서 제안한 개선된 DES의 병렬 파이프라인구조는 키 데이터 같은 소량의 데이터를 암호화하는 것보다는 큰 파일 또는 네트워크의 데이터를 암호화하는데 더욱 효율이 높다.

<표 1>은 클록 속도에 따른 처리블록별 암호화 속도를 보여준다. 이 표에서 알 수 있듯이 처리할 블록이 10000블록(117KB)일 경우,

(350M/(83+9999))*10000*96 ≈ 33.33Gbps

의 암호화 속도를 얻을 수 있다.

표 1. 암호화 처리속도
Table 1. Encryption processing speed

입력클록	암호화 처리속도		
	40블록	83블록	10000블록
10 MHz	314.7Mbps	483Mbps	952Mbps
50 MHz	1.57Gbps	2.42Gbps	4.76Gbps
100 MHz	3.15Gbps	4.83Gbps	9.5Gpbs
350 MHz	11Gbps	16.7Gbps	33.33Gbps

<표 2>는 일반적인 암호화 알고리즘을 소프트웨어로 구현한 것과 하드웨어로 구현한 것에 대한 비교를 나타내고 있다. 소프트웨어 구현의 경우 인텔 기반의 PC에서 재작성 된 코드로 수행한 결과이다.

<표 2>에서 비교한 바와 같이 개선된 DES의 병렬 파이프라인 구조가 기존의 다른 구조의 설계에 비하여 23~550배 이상으로 성능이 향상되었다.

표 2. 암호기의 소프트웨어 및 하드웨어 구현별 비교
Table 2. Comparison for implementation of S/W and H/W cipher

	구현1 [10,11,12]	구현2 [13]	구현3 [14]	구현4
속도 /입력클록	40~60Mbps /200MHz	1.17Gbps /350MHz	1.4Gbps /350MHz	33.33Gbps /350MHz

구현1 : 일반적인 소프트웨어 구현
구현2 : 고속 설계된 소프트웨어 구현
구현3 : 일반적인 하드웨어 구현
구현4 : 병렬 파이프라인 하드웨어 구현

Ⅵ. 결 론

인터넷이나 무선전화, FAX 등과 같이 전송매체에 의한 정보의 양은 급격히 증가하고 있으며 프라이버시의 침해나 허가되지 않은 접근에 의한 공격도 또한 급격히 증가하고 있다. 따라서 이것을 해결하기 위한 보다 완벽한 방법으로는 암호 알고리즘으로 처리하는 것이다.

따라서 본 논문에서는 암호분석의 평가지표에 따라 DES의 비도를 증가시킨 개선된 DES를 효율적인 하드웨어 구조로 설계하기 위하여 고속 병렬파이프라인 구조를 제안하였다. 또한 이것을 VHDL을 이용하여 구현함으로써 고속의 암호기를 설계하였고 설계된 암호기를 시뮬레이션 함으로써 정상적으로 암복호화가 이루어짐을 확인하였다. 설계회로의 시뮬레이션결과 본 암호기는 350MHz 클록 입력에서 33.33Gbps의 암호화 속도를 나타내었다.

병렬 파이프라인 구조에 따른 내부회로의 크기 증가는 현재의 ASIC제조기술의 발달에 의해 칩으로 구현 가능하나 데이터의 입력 및 키의 입력을 위한 pad가 너무 크게 되므로 칩의 크기에 제한을 받게되고, 칩에 사용되는 총 8종의 계수(E, S, P, IP, FP, PC-1, PC-2, SR table)값이 고정될 경우 칩 구조의 분석이 용이해지게 되므로 계수값을 PROM의 형태로 제작하는 등의 동적설계가 필요하며, 이를 위한 입출력 pad의 증가는 현실적인 문제로 남는다. 따라서 개선된 DES의 비도와 밀접한 관계가 있는 S-box만을 동적설계 하는 등의 현실적인 응용을 위한 구조 변경이 필요하겠다.

본 논문의 결과는 급속히 초고속화 되어가고 있는 컴퓨터 통신망에서 비인가자에 대한 전송정보의 보호에 효과적으로 적용되어질 수 있을 것이다.

참 고 문 헌

[1] S. J. Han, "The Improvement Data Encryption Standard(DES) Algorithm," Proceedings of ISSSTA'96, IEEE, Vol.3, No.3, pp.1167-1170, Sept. 1996.

[2] S. J. Han, "Improved-DES Cryptosystem Design," Journal of KISS, Vol.24, No.1, pp.57-67, Jan. 1997.

[3] Schneirer Bruce, *Applied Cryptography*, John Wiley & Sons, Inc., pp.219-296, 1988.

[4] E. Biham and A. Shamir, "Differential Cryptanalysis of DES-like Cryptosystems," Journal of Cryptology, Vol.4, No.1, pp.3-72, 1991

[5] NBS, *Data Encryption Standard*, Federal

Information Processing Standard Pub. No. 46, Jan. 1977

[6] J. B. Kam & G. I. Davida, "Structured Design of Substitution Permutation Encryption Networks," IEEE Trans. on Comput., Vol.28, No.10, pp.747-753, Oct. 1989.

[7] A. F. Webster, & S. E. Tavares, "On the design of S-boxes," CRYPTO '85, 1985.

[8] Frank Hoornaert, Jo Goubert, and Yvo Desmedt, "Efficient hardware implementation of the DES," Journal of Cryptology, Vol.4, No.1, pp.148-151, 1987

[9] Ingrid Verbauwhede, Frank Hoornaert, Joos Vandewalle, and Hugo DeMan, "Security Considerations in the Design and Implementation of a new DES chip," Eurocrypt'87, 1987

[10] Deborah Williams and Harvey J. Hindin, "*Can software do encryption job?*," Electronics, 1980.7

[11] Andreas Pfitzmann and Ralf Abmann, "Efficient Software Implementations of (Generalized)DES," SECURICOM '90, 1990.

[12] Ralph C. Merkle, "Fast Software Functions," CRYPTO '90, 1990.

[13] T. K. Park & D. J. Hwang, "A Pipelined Architecture for the High-Speed Encryption of DES," Journal of The Korean Institute of Information Security and Cryptology, Vol.3, No.2, pp.41-51, 1993.

[14] Hans Eberle, "A High-speed DES Implementation for Network Applications," CRYPTO'92, 1992.

최 광 윤(Kwang-Yun Choi) 정회원

1998년 : 조선대학교 컴퓨터공학과 학사

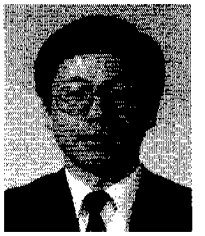
1998년 2월~현재 : 조선대학교 전자공학과 석사과정 (조선대학교 수송계 부품공장자동화 연구센터 연구원)

<주관심분야> 통신보안시스템설계, 네트워크보안, 음성합성, ASIC설계

정 일 용(Il-Yong Chung) 정회원

22권 12호 참조

한 승 조(Seung-Jo Han) 정회원



1980 : 조선대학교 전자공학과 학사

1982년 : 조선대학교 대학원 전자공학과석사

1994 : 충북대학교 대학원 전자계산학과 박사

1997년 : 조선대학교 전자·정보통신공학부 교수

1986년 6월~1987년 3월 : Univ. of New Oleans 객원교수

1996년 2월~1996년 1월 : Univ. of Texas 객원교수

<주관심분야> 통신보안시스템설계, 네트워크보안, 음성합성, ASIC설계